WE CLAIM:

1. A secure component-based operating process including:

(a) retrieving at least one component;

(b) retrieving a record that specifies a component assembly;

(c) checking said component and/or said record for validity;

(d) using said component to form said component assembly in accordance with said record; and

(e) performing a process based at least in part on said component assembly.

2. A process as in claim 1 wherein said step (c) comprises executing said component assembly.

3. A process as in claim 1 wherein said component comprises executable code.

4. A process as in claim 1 wherein said component comprises a load module.

5. A process as in claim 1 wherein:

said record comprises:

(i) directions for assembling said component assembly; and

(ii) information that at least in part specifies a control; and

said process further comprises controlling said step (d) and/or said step (e) based at least in part on said control.

6. A process as in claim 1 wherein said component has a security wrapper, and said controlling step comprises selectively

data indicating that a given movie, song, channel, game, etc. was R rated and allowing a parent to restrict viewing or listening). Such a control location may, for example, also gather information on consumption of water, gas, electricity, telephone usage, etc. (either through use of PPEs 650 integrated in control means for measuring and/or controlling such consumption, or through one or more signals generated by non-VDE systems and delivered to a VDE secure subsystem, for example, for processing, usage control (e.g. usage limiting), and/or billing), transmit such information to one or more utilities, pay for such consumption using VDE secured electronic currency and/or credit, etc.

In addition, one or more budgets for usage could be managed by VDE which would prevent improper, excessive use of a certain, leased appliance, that might, for example lead to failure of the appliance, such as making far more copies using a photocopier than specified by the duty cycle. Such improper use could result in a message, for example on a display panel or television screen, or in the form of a communication from a central clearinghouse, that the user should upgrade to a more robust model.

While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

opening said security wrapper based at least in part on said control.

7. A process as in claim 1 wherein:

said permissions record includes at least one decryption key; and

said controlling step includes controlling use of said decryption key.

8. A process as in claim 1 including performing at least two of said steps (a) and (e) within a protected processing environment.

9. A process as in claim 1 including performing at least two of said steps (a) and (e) at least in part within tamper-resistant hardware.

10. A method as in claim 1 wherein said performing step (e) includes metering usage.

11. A method as in claim 1 wherein said performing step (e) includes auditing usage.

12. A method as in claim 1 wherein said performing step (e) includes budgeting usage.

13. A secure component operating system process including:

receiving a component;

receiving directions specifying use of said component to form a component assembly;

authenticating said received component and/or said directions;

forming, using said component, said component assembly based at least in part on said received directions; and

using said component assembly to perform at least one operation.

14. A method comprising performing the following steps within a secure operating system environment:

providing code;

providing directions specifying assembly of said code into an executable program;

checking said received code and/or said assembly directors for validity; and

in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.

15. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second controls; and

securely applying said first and second controls to manage said resource for use with said data item.

16. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:

(a) securely delivering a first procedure to said electronic arrangement;

(b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;

(c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and

(d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.

17. A method as in claim 16 including performing said delivering step (b) at a time different from the time said delivering step (a) is performed.

18. A method as in claim 16 wherein said step (a) includes delivering said first procedure from a first source, and said step (b) includes delivering said second procedure from a second source different from said first source.

19. A method as in claim 16 further including ensuring the integrity of said first and second procedures.

20. A method as in claim 16 further including validating each of said first and second procedures.

21. A method as in claim 16 further including authenticating each of said first and second procedures.

22. A method as in claim 16 wherein said using step (c) includes executing at least one of said first and second procedures within a tamper-resistant environment.

23. A method as in claim 16 wherein said step (c) includes the step of controlling said data item with at least one of said first and second procedures.

24. A method as in claim 16 further including establishing a relationship between at least one of said first and second procedures and said data item.

25. A method as in claim 16 further including establishing correspondence between said data item and at least one of said first and second procedures.

26. A method as in claim 16 wherein said delivering step (b) comprises delivering at least one load module encrypted at least in part.

27. A method as in claim 26 wherein said delivering step (a) comprises delivering at least one further load module encrypted at least in part.

28. A method as in claim 16 wherein said delivering step (b) comprises delivering at least one content container carrying at least in part encrypted control information.

29. A method as in claim 16 wherein said delivering step (b) comprises delivering a control method and at least one further method.

30. A method as in claim 16 wherein said delivering step (a) includes:

encrypting at least a portion of said first procedure,

communicating said at least in part encrypted first procedure to said electronic arrangement,

decrypting at least a portion of said first procedure at least in part using said electronic arrangement, and

validating said first procedure with said electronic arrangement.

31. A method as in claim 16 wherein said delivering step (b) includes delivering at least one of said first and second procedures within an administrative object.

32. A method as in claim 16 wherein said delivering step (b) includes codelivering said second procedure in at least in part encrypted form with said data item.

33. A method as in claim 16 wherein said performing step includes metering usage.

34. A method as in claim 16 wherein said performing step includes auditing usage.

35. A method as in claim 16 wherein said performing step includes budgeting usage.

36. A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:

(a) selecting an item that is protected with respect to at least one operation;

(b) securely independently delivering plural separate procedures to said electronic appliance;

(c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and

(d) conditioning successful completion of said operation on said delivering step (b) having occurred.

37. A method for processing based on independent deliverables comprising:

securely delivering a first piece of code defining a first part of a process;

separately, securely delivering a second piece of code defining a second part of said process;

ensuring the integrity of the first and second delivered pieces of code; and

performing said process based at least in part on said first and second delivered code pieces.

38. A method as in claim 37 wherein a first piece of code for said process at least in part controls decrypting content.

39. A method as in claim 37 wherein said ensuring step includes validating said first and second pieces of code.

40. A method as in claim 37 wherein said ensuring step includes validating said first and second pieces of code relative to one another.

41. A method as in claim 37 wherein said performing step includes metering usage.

42. A method as in claim 37 wherein said performing step includes auditing activities.

43. A method as in claim 37 wherein said performing step includes budgeting usage.

44. A method as in claim 37 wherein said performing step includes electronically processing content based on electronic controls.

45. A method of securely controlling at least one protected operation with respect to a data item comprising:

(a) supplying at least a first control from a first party;

(b) supplying at least a second control from a second party different from said first party;

(c) securely combining said first and second controls to form a set of controls;

(d) securely associating said control set with said data item; and

(e) securely controlling at least one protected operation with respect to said data item based on said control set.

46. A method as in claim 45 wherein said data item is protected.

47 A method as in claim 45 wherein at least one of said plural controls includes a control relating to metering at least one aspect of use of said protected data item.

48. A method as in claim 45 wherein at least one of said plural controls include a control relating to budgeting at least one aspect of use of said protected data item.

49. A secure method for combining data items into a composite data item comprising:

(a) securely providing a first data item having at least a first control associated therewith;

(b) securely providing a second data item having at least a second control associated therewith;

(c) forming a composite of said first and second data items;

(d) securely combining said first and second controls into a composite control set; and

(e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.

50. A method as in claim 49 wherein said combining step includes preserving each of said first and second controls in said composite set.

51. A method as in claim 49 wherein said performing step comprises governing the operation on said composite of said first

and second data items in accordance with said first control and said second control .

52. A method as in claim 49 wherein said providing step includes ensuring the integrity of said association between said first controls and said first data item is maintained during at least one of transmission, storage and processing of said first data item.

53. A method as in claim 49 wherein said providing step comprises delivering said first data item separately from said first control .

54. A method as in claim 49 wherein said providing step comprises codelivering said first data item and said first control .

55. A secure method for controlling a protected operation comprising:

(a) delivering at least a first control and a second control; and

(b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:

resolving at least one conflict between said first and second controls based on a predefined order;

providing an interaction with a user to form said combination; and

dynamically negotating between said first and second controls.

56. A method as in claim 55 wherein said controlling step (b) includes controlling decryption of electronic content.

57. A method as in claim 55 further including:

receiving protected electronic content from a party; and

authenticating the identity of said party prior to using said received protected electronic content.

58. A secure method comprising:

selecting protected data;

extracting said protected data from an object;

identifying at least one control to manage at least one aspect of use of said extracted data;

placing said extracted data into a further object; and

associating said at least one control with said further object.

59. A method as in claim 58 further including limiting at least one aspect of use of said further object based on said at least one control.

60. A secure method of modifying a protected object comprising:

(a) providing a protected object; and

(b) embedding at least one additional element into said protected object without unprotecting said object.

61. A method as in claim 60 further including:

associating at least one control with said object; and

limiting usage of said element in accordance with said control.

62. A method as in claim 60 further including including a permissions record within said object.

63. A method as in claim 61 further including at least in part encrypting said object.

64. A method for managing at least one resource with a secure operating environment, said method comprising:

securely receiving a first load module from a first entity external to said operating environment;

securely receiving a second load module from a second entity external to said operating environment, said second entity being different from said first entity;

securely processing, using at least one resource, a data item associated with said first and second load modules; and

securely applying said first and second load modules to manage said resource for use with said data item.

65. A method for negotiating electronic contracts, comprising:

receiving a first control set from a remote site;

providing a second control set;

performing, within a protected processing environment, an electronic negotiation between said first control set and said second control set, including providing interaction between said first and second control sets; and

producing a negotiated control set resulting from said interaction between said first and second control sets.

66. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

67. A system for supporting electronic commerce including:

means for creating a first secure control set at a first location;

means for creating a second secure control set at a second location;

means for securely communicating said first secure control set from said first location to said second location; and

negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.

68. A system as in claim 67 further including means for controlling use by a user of protected information content based on at least a portion of said first and/or second control sets.

69. A system as in claim 67 further including means for charging for at least a part of said content use.

70. A secure component-based operating system including:

component retrieving means for retrieving at least one component;

record retrieving means for retrieving a record that specifies a component assembly;

checking means, coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;

using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and

performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

71. A secure component-based operating system including:

a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;

an authenticating manager that checks said component and/or said record for validity;

a channel manager that uses said component to form said component assembly in accordance with said record; and

an execution manager that performs a process based at least in part on said component assembly.

72. A secure component operating system including:

means for receiving a component;

means for receiving directions specifying use of said component to form a component assembly;

means, coupled to said receiving means, for authenticating said received component and/or said directions;

means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and

means, coupled to said forming means, for using said component assembly to perform at least one operation.

73. A secure component operating environment including:

a storage device that stores a component and directions specifying use of said component to form a component assembly;

an authenticating manager that authenticates said component and/or said directions;

a channel manager that forms, using said component, said component assembly based at least in part on said directions; and

a channel that executes said component assembly to perform at least one operation.

74. A secure operating system environment comprising:

a storage device that stores code and directors specifying assembly of said code into an executable program;

a validating device that checks said received code and/or said assembly directors for validity; and

an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.

75. A secure operating environment system for managing at least one resource comprising:

a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and

a protected processing environment, coupled to said communications arrangement, that:

(a) securely processes, using at least one resource, a data item associated with said first and second controls, and

(b) securely applies said first and second controls to manage said resource for use of said data item.

76. A system for negotiating electronic contracts, comprising:

a storage arrangement that that stores a first control set received from a remote site, and stores a second control set;

a protected processing environment, coupled to said storage arrangement, that:

(a) performs an electronic negotiation between said first control set and said second control set,

(b) provides interaction between said first and second control sets, and

(c) produces a negotiated control set resulting from said interaction between said first and second control sets.

77. A system as in claim 76 further including means for electronically enforcing said negotiated control set.

78. A system as in claim 76 further including means for generating an electronic contract based on said negotiated control set.

79. A method for supporting electronic commerce including:

creating a first secure control set at a first location;

creating a second secure control set at a second location;

securely communicating said first secure control set from said first location to said second location; and

electronically negotiating, at said second location, an electronic contract, including the step of securely executing at least a portion of said first and second secure control sets.

80. An electronic appliance comprising:

a processor; and

at least one memory device connected to said processor;

wherein said processor includes:

retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory device,

checking means coupled to said retrieving means for checking siad component and/or said record for validity, and

using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record.

81. An electronic appliance comprising:

at least one processor;

at least one memory device connected to said processor; and

at least one input/output connection coupled to said processor,

wherein said processor at least in part executes a rights operating system to provide a secure operating environment within said electronic appliance.

82. An electronic appliance as in claim 81 wherein said processor includes means for providing a channel, said channel assembling independently deliverable components into a component assembly and executing said component assembly.

83. An electronic appliance as in claim 81 further including a secondary storage device coupled to said processor, said secondary storage device storing a secure database, said processor including means for decryting information obtained from said secure database and for encrypting information to be written to said secure database.

84. An electronic appliance as in claim 81 wherein said processor and said memory device are disposed in a secure, tamper-resistance encapsulation.

85. An electronic appliance as in claim 81 wherein said processor includes a hardware encryptor/decryptor.

86. An electronic appliance as in claim 81 wherein said processor includes a real time clock.

87. An electronic appliance as in claim 81 wherein said processor includes a random number generator.

88. An electronic appliance as in claim 81 wherein said memory device stores audit information.

89. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving a first control from a first entity external to said operating environment;

securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;

using at least one resource;

securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

90. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:

securely receiving first and second control alternatives from an entity external to said operating environment;

selecting one of said first and second control alternatives;

using at least one resource;

if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and

if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

Add a2